UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/510,911	05/02/2005	Stefan Axelsson	P16321-US1	2070

27045 7590 12/10/2008
ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)	
Office Action Summary	10/510,911	AXELSSON, STEFAN	
	Examiner	**Art Unit**	
	AREZOO SHERKAT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08 October 2004_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-9_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-9_ is/are rejected.

7)☒ Claim(s) _1-9_ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _10/8/2004_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

Claims 1-9 are presented for examination.

Throughout this office action, Examiner has included references to particular sections of the prior art(s) for Applicant's convenience. Although the specified citations are representative of the teachings in the prior art(s) as applicable to each specific limitation, other passages and/or figures may apply as well. Therefore, in preparing the response, Applicant is respectfully requested to consider each prior art in its entirety, as well as the specific citation(s)/passage(s) cited by the Examiner for teachings corresponding to all or part(s) of the claimed invention.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 10/8/2004 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Claim Objections

Claims 1-9 are objected to because of the following informalities:

Claim 1 recites the limitation "the given filename" in the third line of the body of the claim and "the secret value” in the last line of the body of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation "the given filename" in the third line of the body of the claim and "the secret value” in the 10th and 13th line of the body of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitation "the filename" in the first line of the body of the claim and “the secret value” on the third and fifth lines. There is insufficient antecedent basis for this limitation in the claim.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 7 and 8 are rejected under 35 U.S.C. 112, second paragraph, as being unclear as to whether it is applicant's intention to claim “a system” or "a method”, i.e., claims 7 and 8 are not clearly directed to either an apparatus or a method.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono, (U.S. Patent No. 6,643,773), in view of Castro et al., (U.S. Patent No. 6,671,821 and Castro hereinafter).

Regarding claims 1, 3, and 9, Hardjono discloses a method of authentication, wherein a plurality of nodes communicate in a multicast, whereby the sending node and the receiving node share a common secret value and thereby belong to an accepted group (col. 4, lines 27-67 and col. 5, lines 1-67 and col. 6, lines 1-43)("*It should be noted, that the terms client and server could amount to any two parties involved in a communication session and that the terms filename and file could amount to virtually any type of information on any format such as data files or packets of data*")(par. 20 of the published disclosure of the instant application), comprising the steps of:

Hardjono discloses wherein upon initiating a multicast, a symmetrical shared multicast encryption key (i.e., shared key) is distributed to each descendant router in the multicast. The shared key and the hash function is then used to determine if the tag (i.e., hash) falls within the specified examination guidelines and the message is authentic. Therefore, Hardjono's message/data packet, explicitly contains the message and message's tag. It is known in the art to include timestamps in the data packet to prevent replay attacks (i.e., wherein the message corresponds to the filename/file, and a tag including data indicating that the receiving node is in the multicast corresponds to a first hash value according to a first hash function formed from the filename and the secret value)(col. 4, lines 27-67 and col. 5, lines 1-67 and col. 6, lines 1-43).

Hardjono does not explicitly disclose a nonce which is associated with the given filename.

However, Castro discloses adding the variable t, a timestamp or a counter, in the message, which is used to prevent replay attacks (col. 13, lines 4-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Hardjono with teachings of Castro because it would allow adding the variable t, a timestamp or a counter, in the message as disclosed by Castro. One of ordinary skill in the art would have been motivated by the suggestion of Castro to prevent replay attacks (Castro, col. 13, lines 4-20).

Regarding claims 2, 4, and 8, Hardjono discloses the step of:

extracting the filename/file of a received first message, extracting the first hash value (i.e., wherein the receiving router inherently has to extract the message, corresponding to the filename/file, and the base tag, corresponding to the first hash value, before it can determine whether or not the message is authentic – note that the instant application explicitly discloses " the terms filename and file could amount to virtually any type of information on any format such as data files or packets of data" - par. 20 of the published disclosure),

forming a value of the received filename and the secret value (i.e., the receiving router generates and appends an upstream tag to the message/base tag combination, wherein the message/base tag combination corresponds to the value formed of the received filename and the secret value),

forming a second hash value according to the first hash function formed from the value of the filename and the secret value (i.e., the receiving router generates and appends an upstream tag to the message/base tag combination, wherein the upstream tag corresponds to the second hash value. In addition, the router ID number of the receiving router also is appended to the message/base tag combination. The upstream tag is a function of the message, receiving router ID number, base tag, and encryption key of the receiving router. Each of these parameters may be used as input into a key hash function to produce the upstream tag, and the key hash function is the same for all tags. After the upstream tag and router ID number are appended to the message/base tag combination, the entire message combination is transmitted to the receiving router's parent router (step 214)),

comparing the first hash value with the second hash value and if the values are the same (i.e., wherein at each receiving node if message is determined to be authentic), establishing that the first message stems from a client belonging to the accepted group, otherwise establishing that the client does not belong to the accepted group (i.e., As discussed in FIG. 3, use of the receiving router encryption key enables it's parent to confirm that it in fact received the message from the receiving router. In another word, if the authentication is confirmed, then it is confirmed that the message is received from a network device in the multicast)(col. 5, lines 25-67 and col. 6 lines 1-67 and col. 7, lines 1-26).

Hardjono does not explicitly disclose a nonce which is associated with the given filename.

However, Castro discloses adding the variable t, a timestamp or a counter, in the message, which is used to prevent replay attacks (col. 13, lines 4-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Hardjono with teachings of Castro because it would allow adding the variable t, a timestamp or a counter, in the message as disclosed by Castro. One of ordinary skill in the art would have been motivated by the suggestion of Castro to prevent replay attacks (Castro, col. 13, lines 4-20).

Regarding claim 5, Hardjono discloses a method according to claim 3, wherein the first hash function is the same as the second hash function (i.e., the key of each router in a multicast is generated as a function of the root key, wherein a router can determine the key of any given descendant router by iteratively utilizing the (same) hash function to calculate each lineally successive downstream child router between it and a give descendant router)(col. 5, lines 5-21).

Regarding claim 6, Hardjono discloses a method according to claim 1, wherein the inputs to hash functions are concatenated (i.e., The upstream tag is a function of the message, receiving router ID number, base tag, and encryption key of the receiving router wherein it is inherent that multiple parameters as inputs to the hash function are concatenated/combined).

Regarding claim 7, since claim 7 has combined limitations of claims 1 and 4; therefore, the logic relied upon for rejecting claim 1 combined with the reasoning for rejection of claim 4 as discussed above is applicable in rejecting claim 7.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Please see the attached PTO-892 for a complete listing.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AREZOO SHERKAT whose telephone number is (571)272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Arezoo Sherkat/
Patent Examiner
Group 2431
Nov. 12, 2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432